UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/597,134	07/12/2006	Padraig Moran	149702.00001	6515

25207   7590   07/21/2009
BRYAN CAVE POWELL GOLDSTEIN
ONE ATLANTIC CENTER FOURTEENTH FLOOR
1201 WEST PEACHTREE STREET NW
ATLANTA, GA 30309-3488

EXAMINER
FIALKOWSKI, MICHAEL R

ART UNIT	PAPER NUMBER
2419	

MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

This office action is in response to an amendment filed on March 23 2009.

Claims 1-7,9-13, and 15 are pending with Claims 8 and 14 being cancelled.

Claim Objections

1.   Claim 12 is objected to because of the following informalities:

Re claim 12, Applicant recites on line 2 in part, "access to the internal Mobile IP

home agent". Examiner suggests changing to, "access to the Internal Mobile IP Home

Agent" to match antecedence.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

1.   Claims 1,3-7,9-11,15 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Liu et al (2004/0120295) in view of Leung et al (2003/0224788) & Joy et al

(2004/0268357).

Re claim 1, Liu et al discloses a module for providing in a Mobile Virtual Private network mobility for a remotely connected node moving between an external network and an internal network, the module comprising:

a mobile agent device (VPN gateway / MIP - Mobile IP proxy), the mobile agent adapted for:

a. termination of Mobile IP tunnel (See Figure 2B, label 242) from a remotely connecting Mobile Node (mobile node);

b. termination of an IPSec VPN tunnel (See Figure 2B, label 248) from the remotely connecting Mobile Node, the IPSec VPN tunnel used for tunneling to the mobile agent traffic intended for a destination node within the internal network;;

c. dynamic selection of Internal Mobile IP Home Agent (home agent) based on user authentication (associates mobile node with home agent by binding addresses [0042]-[0043]);

d. direct routing of the traffic from the mobile agent towards the destination node ([0051]).

Liu et al does not explicitly disclose a mobile agent device positioned at the ends of the internal network and wherein the mobile agent device stores in a mapping table a traffic encapsulation type used for routing traffic from the mobile agent to the Internal Mobile IP Home Agent; and tunneling of the traffic between the mobile agent and the selected Internal Mobile IP Home Agent prior to routing of the traffic from the selected Internal Mobile IP Home Agent toward the destination node and provision of extended authentication, after Mobile IP connection establishment, and during the VPN

negotiation phase, based on extra user credentials, or a one-time-password

mechanism..

However, Leung et al teaches of a mobile agent device (MIP proxy 345) positioned at

the ends of the internal network (for example, in Figure 3 MIP proxy is located at the

end of the internal network) and tunneling of the traffic between the mobile agent and

the selected Internal Mobile IP Home Agent (MIP proxy forms a tunnel to the home

agent [0053]) prior to routing of the traffic from the selected Internal Mobile IP Home

Agent toward the destination node (for example, corresponding node in Figure 1) and

provisioning extended authentication (authentication [0036]), after Mobile IP connection

establishment (registration request [0034]-[0035]), and during the VPN negotiation

phase (for example, setting up a tunnel [0030]), based on extra user credentials (for

example, a Network Access Identifier ([0036]), or a one-time-password mechanism. It

would have been obvious for one of ordinary skill in the art at the time of the invention to

position the mobile agent device at the end of the internal network, to tunnel the traffic

between the mobile agent and the home agent, and provide authentication as taught by

Leung et al in the module of Liu et al in order to provide extra security by use of tunnels

and authentication in an internal network.

Leung et al does not explicitly teach wherein the mobile agent device stores in a

mapping table a traffic encapsulation type used for routing traffic from the mobile agent

to the Internal Mobile IP Home Agent. However, Joy et al teaches of a device

(forwarder) which stores in a mapping table (mapping table) an encapsulation type

(encapsulation mapping entry) used for routing traffic from a device to another that are

tunneling traffic (See Figure 38, [0358], [0406]-[0420]). It would have been obvious for one of ordinary skill in the art at the time of the invention to include a mapping table as taught by Joy et al in the module of Liu et al in order to keep track of which streams should be tunneled versus regular traffic.

Re claim 3, note that Liu et al discloses the module wherein the mobile agent device appears as a Mobile IP Home Agent (home agent) towards the remotely connecting Mobile Node (mobile node) (includes a home agent module that emulates a home agent for mobile nodes [0028]).

Re claim 4, note that Liu et al discloses the module wherein the mobile agent device (Foreign Agent module in MIP proxy) provides a dynamically assigned Mobile IP address (care-of address) to the remotely connecting Mobile Node (via DHCP) , if requested to do so by the remotely connecting Mobile Node (mobile node uses DHCP) ([0024] [0031], for registering with MIP proxy).

Re claim 5, note that Liu et al discloses the module wherein the mobile agent device provides a termination point (data tunnel is created between mobile node and MIP proxy) for IKE (Security Association may be created using IKE [0031]) & IPSec VPN connections (See Figure 2B, label 248) from a remotely connecting Mobile Node.

Re claim 6, Liu et al modified by Leung et al & Joy et al teaches the module of claim 1 as stated above, but does explicitly disclose wherein the traffic encapsulation type set in the mapping table is IP encapsulation. However, Leung et al teaches IP encapsulated (IP-in-IP) tunneling is used for transfer of traffic between the mobile agent device (care of address, which is for example MIP proxy) and the Internal Home Agent

(home agent) ([0043]). It would have been obvious for one of ordinary skill in the art at

the time of the invention in the area of mobile networks to include IP encapsulation to

transfer the traffic between nodes as taught by Leung et al in the device of Liu et al in

order to set up communication in a Mobile IP standard (Leung et al [0043]).

Re claim 7, Liu et al modified by Leung et al & Joy et al teaches the module of

claim 1 as stated above, but does explicitly disclose wherein the traffic encapsulation

type set in the mapping table is UDP encapsulation. However, Leung et al teaches UDP

encapsulated (IP-UDP) tunneling is used for transfer of traffic between the mobile agent

device (MIP proxy) and the Internal Home Agent (Internal Home Agent) (extension

indicates tunnel mode as IP-UDP or IP-IP [0045]) . It would have been obvious for one

of ordinary skill in the art at the time of the invention in the area of mobile networks to

include UDP encapsulation to transfer the traffic between nodes as taught by Leung et

al in the device of Liu et al in order to communicate through a NAT (Leung et al [0040]).

Re claim 9, Liu et al modified by Leung et al & Joy et al teaches the module of

claim 1 as stated above, but does explicitly disclose wherein IP encapsulated tunneling

is used for transfer of traffic between the remotely connecting Mobile Node and the

mobile agent device. However, Leung et al teaches IP encapsulated (IP –in-IP)

tunneling is used for transfer of traffic between the remotely connecting Mobile Node

and the mobile agent device (MIP proxy) ([0055]). It would have been obvious for one of

ordinary skill in the art at the time of the invention in the area of mobile networks to

include IP encapsulation to transfer the traffic between nodes as taught by Leung et al

in the device of Liu et al in order to set up communication in a Mobile IP standard
(Leung et al [0043]).

Re claim 10, Liu et al modified by Leung et al & Joy et al teaches the device of
claim 1 as stated above, but does not explicitly disclose wherein UDP encapsulated
tunneling is used for transfer of traffic between the remotely connecting Mobile Node
and the mobile agent device. However, Leung et al teaches UDP encapsulated (IP–in-
UDP) tunneling is used for transfer of traffic between the remotely connecting Mobile
Node (mobile node) and the mobile agent device (MIP proxy) [0048]. It would have
been obvious for one of ordinary skill in the art at the time of the invention in the area of
mobile networks to include UDP encapsulation to transfer the traffic between nodes as
taught by Leung et al in the module of Liu et al in order to communicate through a NAT
(Leung et al [0040]).

Re claim 11, note that Liu discloses the module wherein IPSec tunneling is used
for protection of the transfer of traffic between the mobile node and the mobile agent
device (VPN gateway) (See Figure 4B, label 450), within said encapsulation (packet is
encapsulated until steps 460,and 465).

Re claim 15, note that Liu discloses the module wherein IPSec tunneling is used
for protection of the transfer of traffic between the remotely connecting Mobile Node and
the mobile agent device (VPN gateway) (See Figure 4B, label 450), within said
encapsulation (packet is encapsulated until steps 460,and 465).

2.   Claims 2 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Liu et al in view of Leung et al & Joy et al as applied to claim 1 above, and further in

view of Makineni et al (2002/0066036).

        Re claim 2, Liu et al modified by Leung et al & Joy et al teaches the module of

claim 1 as stated above, but does not explicitly disclose wherein the mobile agent

device appears as a Mobile IP Foreign Agent towards the Internal Mobile IP Home

Agent. However, Makineni et al teaches of a mobile agent device (relay server)

appears as a Mobile IP Foreign Agent (Foreign agent) towards (for communicating

with) the Internal Mobile IP Home Agent (home server) ([0027]). It would have been

obvious for one of ordinary skill in the art at the time of the invention in the area of

mobile networks to include a foreign agent for communicating with the home agent as

taught by Makineni et al in the modified module of Liu et al in order to conform to the

Mobile IP network communication.

        Re claim 12, Liu et al modified by Leung et al & Joy et al teaches the module of

claim 1 as stated above, but does not explicitly disclose comprising restriction of user

access to the internal Mobile IP home agent or internal network, until extended user

authentication is carried out. However, Makineni et al teaches of restriction of user

access (ensures the identity of the client) to the internal Mobile IP home agent or

internal network, until extended user authentication (relay server authenticates

message) is carried out ([0027]). It would have been obvious for one of ordinary skill in

the art at the time of the invention in the area of mobile networks to include restriction of

user access until user authentication is carried out as taught by Makineni et al in the

modified module of Liu et al in order to secure access to an internal network.

5.   Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liu et al

in view of Leung et al & Joy et al as applied to claim 1 above, and further in view of

Chowdhury et al (2004/0106393).

        Re claim 13, Liu et al modified by Leung et al & Joy et al teaches the module of

claim 1 as stated above, but does not explicitly discloses the device further comprising

time and volume based accounting is carried out on a per Mobile Node basis. However,

Chowdhury et al teaches of a device (HAAA) comprising time (time-of-day, session

duration, and timeout lengths) and volume (data volume, data bandwidth) based

accounting (determines, delivers, and enforces) is carried out on a per Mobile Node

(subscriber) basis ([0018]). It would have been obvious for one of ordinary skill in the

art at the time of the invention in the area of mobile networks to include time and volume

accounting as taught by Chowdhury et al in the modified module of Liu et al in order to

enforce different policies based on a mobile node.

Response to Arguments

1.   Applicant's arguments with respect to claims 1-7,9-13, and 15 have been

considered but are moot in view of the new ground(s) of rejection.

Conclusion

1.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL FIALKOWSKI whose telephone number is (571)270-5425. The examiner can normally be reached on Monday - Friday 9:30am-7pm EST, alternating Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Daniel Ryman can be reached on (571)272-3152. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. F./
Examiner, Art Unit 2419

/Daniel J. Ryman/
Supervisory Patent Examiner, Art Unit 2419